WHO WROTE THIS CODE?

PRIVACY GOVERNANCE IN THE AGE OF VIBE CODING

AMBER WELCH

AWS SENIOR ASSURANCE CONSULTANT

HOW DO WE PROTECT PRIVACY IN THE AI ERA?

- I don't know!
- But I have some ideas…
- There are no "best practices" anymore
- Shift focus to process design for identifying errors quickly

WHAT IS PERSONAL DATA?

- Any data related to a real person
- Can be structured or unstructured
- Non-deterministic AI output can create sensitive or incorrect data
- AI agents can act upon personal data in unexpected ways
- Code reviews and agentic design should consider privacy

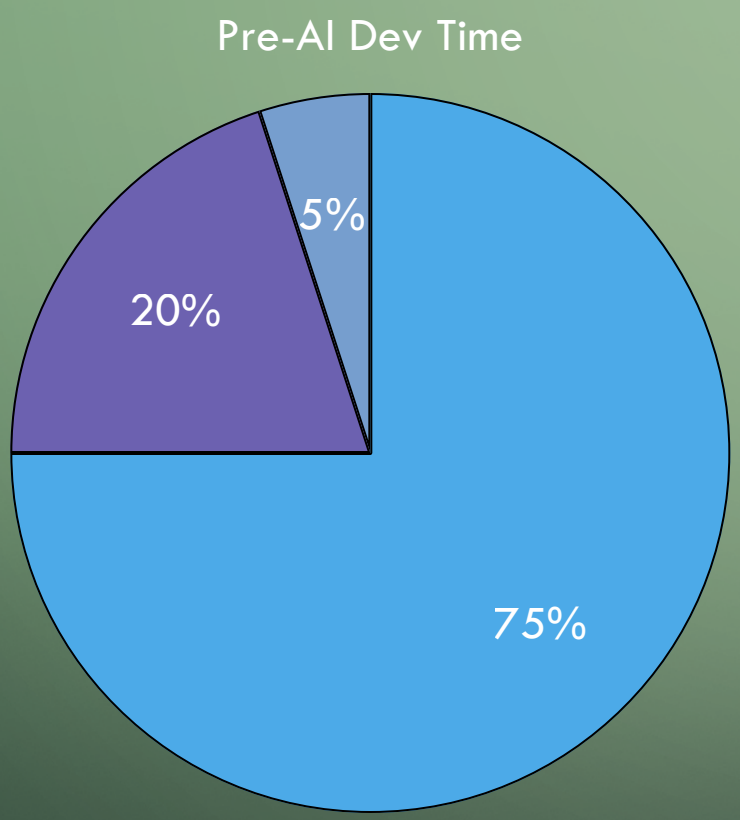
WHAT IS AUTOMATED DECISION MAKING?

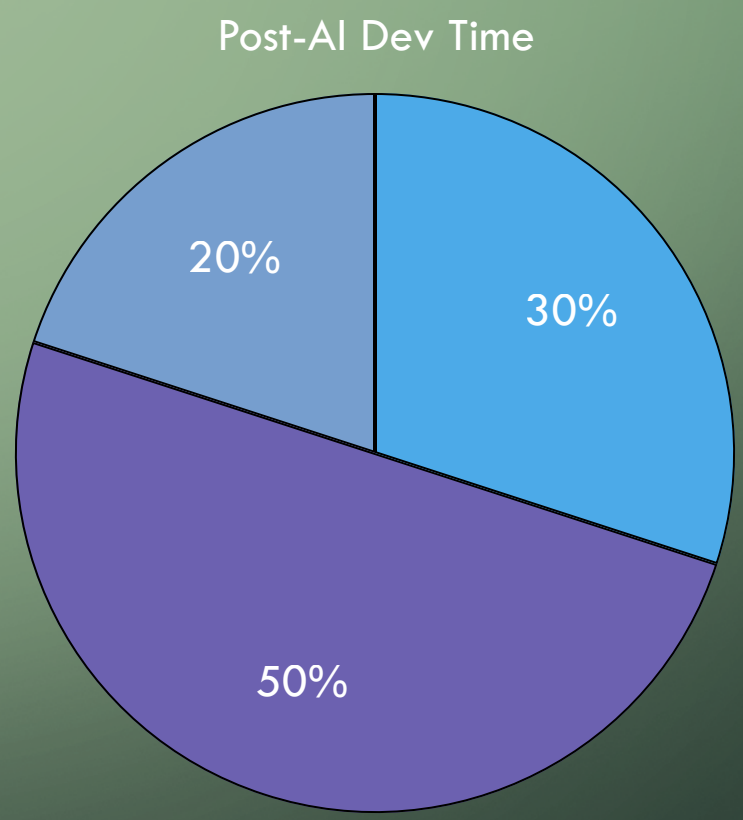
- Can be credit decisions, insurance claims, legal penalties, etc.
- Current explainable AI methods may not meet GDPR Article 22
- Consider allowing automated decisions only for favorable outcomes and requiring human review for unfavorable ones
- For high impact decisions, only use AI to assist human processes
- Be cautious here until there is more guidance and precedent

HOW DO WE REVIEW NEW DEVELOPMENT?

- We still need both senior and junior developers
- With agentic AI, developers become AI team managers
- Require a set percentage of manual coding for skill development
- Don’t release code that the developer cannot explain
- Change the ratio of coding, testing, and training time

HOW CAN WE MAINTAIN TECHNICAL EXPERTISE?





Code Test Train

PRIVACY IN THE AI SUPPLY CHAIN

- There is no “AI exemption” in privacy laws for training models
- Review AI contracts for training and data management clauses
- Train employees to use only approved AI tools with personal data
- Inform customers and end users of AI use in your products

THANK YOU!

AMBER WELCH

AWELCHX@AMAZON.COM
LINKEDIN.COM/IN/AMBERWELCH1